

# XCTF\_easycap

原创

永远是深夜有多好。 于 2022-01-06 15:57:24 发布 1150 收藏

分类专栏: [XCTF](#) 文章标签: [网络](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_37370714/article/details/122345730](https://blog.csdn.net/qq_37370714/article/details/122345730)

版权



[XCTF 专栏收录该内容](#)

17 篇文章 0 订阅

订阅专栏

easycap 11 最佳Writeup由BinPr1me • zh\_cn提供

难度系数: 1.0

题目来源: [bsidessf-ctf-2017](#)

题目描述: 你能从截取的数据包中得到flag吗?

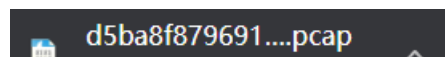
题目场景: 暂无

题目附件: [附件1](#)

CSDN @猫于星空

一星问题应该不大

看了下附件



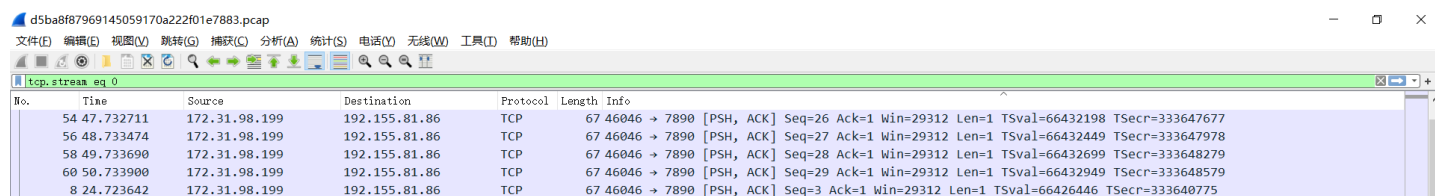
百度了一下.pcap是什么文件

这个抓包库给抓包系统提供了一个高层次的接口。所有网络上的数据包, 甚至是那些发送给其他主机的, 通过这种机制, 都是可以捕获的。

它也支持把捕获的数据包保存为本地文件和从本地文件读取信息。——百度百科

说白了应该就是网络抓包文件格式

用wireshark打开



62	51.734291	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=30	Ack=1	Win=29312	Len=1	TSval=66433199	TSecr=333648893
64	52.734629	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=31	Ack=1	Win=29312	Len=1	TSval=66433449	TSecr=333649182
66	53.734919	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=32	Ack=1	Win=29312	Len=1	TSval=66433699	TSecr=333649480
68	54.735541	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=33	Ack=1	Win=29312	Len=1	TSval=66433949	TSecr=333649778
70	55.735752	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=34	Ack=1	Win=29312	Len=1	TSval=66434199	TSecr=333650080
72	56.736020	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=35	Ack=1	Win=29312	Len=1	TSval=66434449	TSecr=333650379
74	57.736304	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=36	Ack=1	Win=29312	Len=1	TSval=66434699	TSecr=333650679
76	58.736572	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=37	Ack=1	Win=29312	Len=1	TSval=66434949	TSecr=333650979
78	70.450175	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=38	Ack=1	Win=29312	Len=1	TSval=66437878	TSecr=333651279
10	25.724349	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=4	Ack=1	Win=29312	Len=1	TSval=66426696	TSecr=333641076
12	26.724839	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=5	Ack=1	Win=29312	Len=1	TSval=66426946	TSecr=333641376
14	27.725043	172.31.98.199	192.155.81.86	TCP	6746046	→ 7890	[PSH, ACK]	Seq=6	Ack=1	Win=29312	Len=1	TSval=66427196	TSecr=333641676

> Frame 72: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)  
 > Ethernet II, Src: IntelCor\_4b:f0:c3 (e4:b3:18:4b:f0:c3), Dst: ArubaaHe\_c9:7d:7a (9c:1c:12:c9:7d:7a)  
 > Destination: ArubaaHe\_c9:7d:7a (9c:1c:12:c9:7d:7a)  
 > Source: IntelCor\_4b:f0:c3 (e4:b3:18:4b:f0:c3)  
 Type: IPv4 (0x0800)

```

0000  9c 1c 12 c9 7d 7a e4 b3 18 4b f0 c3 08 00 45 00  ...}z...K...E-
0010  00 35 c3 5c 40 00 00 06 56 8e ac 1f 62 c7 c0 9b  -5\@:@:V...b...
0020  51 56 b3 de 1e d2 ae 97 bd 34 fc 98 46 d2 80 18  QV.....4..F...
0030  00 e5 bb d9 00 00 01 01 08 0a 03 f5 b5 91 13 e3  .....
0040  19 cb 30                                     ..0
  
```

d5ba8f87969145059170a222f01e7883.pcap | 分组: 82 · 已显示: 82 (100.0%) CSDN | 猫子星空

发现全是TCP 试试追踪TCP流

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · d5ba8f87969145059170a222f01e7883.pcap

FLAG: 385b87afc8671dee07550290d16a8071

38 客户端 分组, 0 服务器 分组, 0 turn(s).

整个对话 (38 bytes) Show data as ASCII 流 0

查找: 查找下一个 (N)

滤掉此流 打印 另存为... 返回 Close Help

CSDN | 猫子星空

flag: FLAG:385b87afc8671dee07550290d16a8071